

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

### Amendments to the Claims

Please amend and add new claims as indicated below. This listing of claims will replace all prior versions, and listings, of claims in the application:

- 1           1.     (Currently Amended) A method for utilizing a pseudonym for a permanent  
2     key pair, the method comprising:  
3           producing [ a ] the pseudonym for the permanent key pair, the pseudonym  
4     including a public pseudonym key within a platform;  
5           placing the public pseudonym key into a certificate template;  
6           performing a hash operation on the certificate template to produce a certificate  
7     hash value;  
8           performing a transformation on the certificate hash value for transmission from  
9     the platform;  
10          receiving a signed result being a digital signature for the transformed certificate  
11     hash value; [ and ]  
12          performing an inverse transformation on the signed result to recover a digital  
13     signature of the certificate hash value; and  
14          erasing at least the public pseudonym key after utilization in a communication  
15     session.
- 16          2.     (Original) The method of claim 1, wherein the producing of the pseudonym  
17     includes generating the public pseudonym key and a private pseudonym key  
18     corresponding to the public pseudonym key.

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

1           3.     (Original) The method of claim 1, wherein the placing of the public  
2     pseudonym key into the certificate template includes writing the public pseudonym key  
3     into a field of the certificate template.

4           4.     (Original) The method of claim 1, wherein the performing of the  
5     transformation comprises:  
6             performing a logical operation on the certificate hash value using a pseudo-  
7     random number to produce a value differing from the certificate hash value.

8           5.     (Original) The method of claim 4, wherein the pseudo-random number is a  
9     predetermined value raised to an inverse power designated by a pseudo-random value.

10          6.     (Original) The method of claim 5, wherein the pseudo-random value is  
11     stored in secure memory.

12          7.     (Original) The method of claim 4, wherein the performing of the inverse  
13     transformation comprises performing a logical operation on the signed result using an  
14     inverse of the pseudo-random number.

15          8.     (Original) The method of claim 1, wherein prior to receiving the digital  
16     signature, the method comprises:  
17             digitally signing a certification request, including the transformed certificate hash  
18     value, with a private key of a first platform to produce a signed certification request.

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

1           9.     (Original) The method of claim 8, wherein prior to receiving the digital  
2     signature, the method further comprises:  
3           obtaining a device certificate being a digital certificate chain that includes a public  
4     key of a first platform, to accompany the signed certificate request

5           10.    (Original) The method of claim 9, wherein prior to receiving the digital  
6     signature, the method further comprises:  
7           transferring the signed certificate request and the device certificate to a second  
8     platform.

9           11.    (Previously Presented) The method of claim 1 further comprising:  
10     storing the digital signature of the certificate hash value for use in subsequent  
11     communications to a remotely located platform.

12           12.    (Previously Presented) A device comprising:  
13     a processing unit; and  
14     a persistent memory including a first key pair and at least one pseudonym for use  
15     in communications with a remotely located device and in identifying that a platform  
16     containing the device is secure, wherein the at least one pseudonym includes a second  
17     key pair that is erased after a communication session with the remotely located device  
18     has concluded.

19           13-14. (Cancelled)

20           15.    (Original)     The device of claim 12 further comprising:

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

1 a number generator to assist in producing the at least one pseudonym.

2 16. (Currently Amended) A platform comprising:

3 a transceiver; and

4 a device in communication with the transceiver, the device including a persistent  
5 memory to contain

6 a permanent key pair,

7 at least one pseudonym generated internally within the device and

8 a digital signature of a hash value of a digital certificate chain that includes

9 a public pseudonym key of the at least one pseudonym, wherein at least the public

10 pseudonym key is erased after utilization in a communication session.

11 17. (Original) The platform of claim 16, wherein the device further

12 includes:

13 a processing unit to

14 (i) write the public pseudonym key into a certificate template,

15 (ii) perform a hash operation on the certificate template to produce a

16 certificate hash value,

17 (iii) to perform a transformation operation on the certificate hash value.

18 18. (Original) The platform of claim 17, wherein the processing unit of the

19 device further produces a digital signature of at least the transformed certificate hash

20 value using a private key of the permanent key pair.

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

1           19.   (Previously Presented)    The platform of claim 17, wherein the  
2   processing unit of the device further appending a device certificate with the digital  
3   signature of at least the transformed certificate hash value.

4           20.   (Original)    The platform of claim 19, wherein the device certificate is the  
5   digital certificate chain.

6           21.   (Original) A method for utilizing a persistent memory of a device,  
7   comprising:  
8           storing in the persistent memory a first key pair; and  
9           storing in the persistent memory at least one pseudonym for use in  
10   communications with a remotely located device and in identifying that a platform  
11   containing the device is secure, wherein the at least one pseudonym includes a second  
12   key pair that is erased after a communication session with the remotely located device  
13   has concluded.

14          22.   (Original)    The method of claim 21 further comprising:  
15          utilizing a number generator to assist in producing the at least one pseudonym.

16          23.   (New) A machine accessible medium having associated instructions for  
17   utilizing a persistent memory of a device, the instructions, when accessed, result in one  
18   or more machines performing:  
19          storing in the persistent memory a first key pair; and  
20          storing in the persistent memory at least one pseudonym for use in  
21   communications with a remotely located device and in identifying that a platform

Application No. 09/605,605  
Amendment dated July 1, 2004  
Response to Office Action of June 1, 2004

Atty. Docket No. 042390.P7709  
Examiner Darrow, Justin T  
TC/A.U. 2132

1 containing the device is secure, wherein the at least one pseudonym includes a second  
2 key pair that is erased after a communication session with the remotely located device  
3 has concluded.

4 24. (New) The medium of claim 23, wherein the instructions include further  
5 instructions, which when accessed, result in the one or more machines performing:  
6 utilizing a number generator to assist in producing the at least one pseudonym.